REMARKS

Applicant corrected the status of claim 20 to "original" from "currently amended" since claim 20 was not amended in applicant's prior reply.

The examiner objected to Claims 1 and 11 due to informalities. Applicant has amended the claims to correct the informalities.

Applicant has renumbered claims 27-34 as claims 26-33. Applicant will use amended claim numbers in replying to arguments raised by the examiner. Thus, claims referred to by the examiner as claims 27-34 will be referred below as claims 26-33.

The examiner rejected Claims 1-25 and 27-34 (now claims 1-33) under 35 U.S.C. 102(e) as being anticipated by Ioele et al US Patent No. 7,007,299. The examiner stated in regards to claim 1 that:

> **With regards to claim 1, Ioele teaches a device, coupled to physical links between the data center and a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links (Ioele, Figure 1, column 3 lines 25-35, column 4 lines 35-37) and collect statistical information on packets that are sent between a network and the data center for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the links that the provisioned monitor is on (Ioele, column 6 lines 31-46).**

Claim 1 is distinct over Ioele. Ioele fails to describe or suggest a device, placed on selected links in the data center ... that collects statistical information on packets that are sent between a network and the data center for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from links that the provisioned monitor is coupled to. Rather, Ioele discloses:

> **For example, the size of the Internet connections can be at 100 Mbps. FIG. 1 depicts the network security measures for an Internet hosting site 100. The first level of this security comprises routers 110, such as a pair of CISCO 7200 Routers, that limit external access to the network by the type of Internet traffic. The second level of security is maintained by a plurality of firewalls 121 and 122, such as Cyberguard Firewalls, with one as primary and the other as backup. The firewalls 121 and 122 communicate with each other via an interconnection 160, such as an Ethernet or fiber-optic connection. (Ioele Col. 3, lines 25-35)**

> **Any user requests coming from the Internet to any of the hosted sites must first go through this aggregated bandwidth to a main set of network routers 110, which functions as the first level of network security. The routers 110 screen the requests to limit external access to the network of hosted sites by the type of Internet traffic. (Ioele Col. 4, lines 35-37).**

Ioele describes a system and method for providing security to Internet hosting sites. However, nowhere does Ioele disclose a device... disposed to examine traffic entering or leaving that data center on the coupled physical links. In particular, Ioele does not disclose any device that collects statistical information on packets sent between the network and the data center ..., much less that a device that collects statistical information on packets does so for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the links that the provisioned monitor is coupled to.

Ioele addresses denial of service attacks on Internet sites. Ioele discusses network security measures for an Internet hosting site 100. Ioele has a "first level of this security [that] comprises routers 110 ... that limit external access to the network by the type of Internet traffic." Ioele also has a second level of security ... maintained by a plurality of firewalls 121 and 122, ... [that] communicate with each other via an interconnection 160... ." Therefore, Ioele describes a hierarchical arrangement to provide security using routers and firewalls. While Ioele mentions that: "Any user requests coming from the Internet to any of the hosted sites must first go through this aggregated bandwidth to a main set of network routers 110, which functions as the first level of network security" and that: "[T]he routers 110 screen the requests to limit external access to the network of hosted sites by the type of Internet traffic." (Ioele Col. 4, lines 35-37).

Ioele fails to describe or suggest a device... disposed to examine traffic entering or leaving that data center on the coupled physical links that collects statistical information on packets sent between the network and the data center. No mention is made in Ioele of collection of statistical information on packets. Ioele therefore inherently cannot teach that the collection of the statistical information is made by examining traffic as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to.

Ioele proposes that: "The Internet connections to each site are also sufficiently large to prevent flooding attacks. According to an embodiment of the present invention, the size of the Internet connections is based on the load, i.e., the number of users that will be connected to each

site at once, with the size based on ten to fifty times the actual or estimated load." [Ioele Col. 3, lines 19-21]. While this may protect connections from a denial of service attack, applicant's claim 1, is directed to protecting the data center from attacks. The mechanism employed by Ioele (namely sufficiently large connections, as mentioned by Ioele) is substantially different than the claimed arrangement involving a device to examine traffic entering or leaving the data center on the coupled physical links and to collect statistical information on packets.

Claim 2 is further distinct over Ioele since Ioele fails to disclose that the monitoring device is coupled to a control center through a dedicated, private network. Ioele fails to suggest a control center and the teachings of Ioele's device 140 fails to suggest, much less described the control center coupled thought a dedicated, private network.

> **Another level of security is maintained by an operations and event log management system 140, such as Tivoli, which monitors for indication of software, hardware, network and security problems, and other event logs. [Ioele Col, 3, lines 39-43]**

Indeed, Ioele at Col, 4, lines 41-48, discloses that:

> **Although FIG. 1 only shows a network security scheme for a single Internet hosting site, it should be understood from the present disclosure that multiple Internet hosting sites can have their Internet connections aggregated together, with each site having components 121, 122, 131, 132, 140, and 150 function in similar manner; wherein the firewalls 121, 122 of each Internet hosting site are connected to the same routers 110. Thus, the routers 110 are also used to direct approved Internet traffic to the particular Internet hosting site(s) requested by such traffic.**

Clearly, whether in the single or multiple configurations, Ioele teaches that device 140 is connected to the same routers. Accordingly, claim 2 which calls the monitoring device coupled to a control center through a dedicated, private network is neither described nor suggested by Ioele, since there is nothing about the connection of device 140 or the other devices disclosed in Ioele that corresponds to a dedicated, private network.

Claim 3 is distinct over Ioele, since the references fails to teach a communication process that communicates statistics with the control center, and which receives queries or instructions from the control center.

The examiner contends that Ioele's teachings of event logs at Col. 7, lines 37-64 meet these features. Claim 3 requires that the device communicates the statistics to the control center, event logs are not "statistical information on packets" or "statistics" as previously used in claim 3. In order to clarify claim 3, applicant has amended it to call for: "the statistical information on packets" being communicated to the control center.

In addition, Ioele does not describe that the device receives queries from the control center. Rather, Ioele describes that: "Tivoli ensures the continuity of event log data by constantly monitoring the size of all NT event logs. When a log reaches a user-defined threshold, it is transferred to a central management system using a secure store and forward mechanism. Tivoli provides configuration facilities and a browser with extensive filtering to allow ad-hoc queries and printing of centrally stored event logs and event correlation." Thus, in Ioele the query is to the centrally stored logs in the central management system. Ioele does not describe that a device as in claim 1, which is coupled to the physical links, examines traffic entering or leaving that data center, and collects statistical information on packets ... services queries from the control center.

Claim 4 is distinct since Ioele fails to teach that the monitoring device is a gateway device and includes a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack. Rather, Ioele, in the passage relied on by the examiner, discusses an intrusion detection scheme that provides back tracing of addresses. No mention is made of installing filters.

Claim 11 is allowable over Ioele since Ioele fails to teach ... a provisioned monitor, placed on selected links in the data center ... that collects statistical information for a plurality of provisioned customers, which are on links that are downstream from the selected links ... the provisioned monitor maintaining separate counter logs for each provisioned customer and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to.

Ioele fails to teach the provisioned monitor that collects statistical information for provisioned customers on links that are downstream from links that the provisioned monitor is disposed on. Ioele also fails to teach that the provisioned monitor maintains separate counter

logs for each provisioned customer and a global counter log that accounts for all traffic seen on the link ... .

The examiner equates the event data related to originating points of requests, as disclosed in Col. 7, lines 45-46 of Ioele, with the claimed counter logs. Applicant contends that there is no correspondence or equivalence. The event logs taught by Ioele do not corresponding to the claimed counter logs and are neither described as, nor suggested to, be maintained as separate counter logs for each provisioned customer. Ioele also fails to suggest a global counter log that accounts for all traffic seen on the link. Claims 12-23 add additional distinct features, as discussed of record.

Claim 7 distinguishes over Ioele, since Ioele fails to describe or suggest collecting, using a provisioned monitor statistical information on packets that are sent between a network and a plurality of customers of the data center by examining traffic on selected links in the data center as if the collecting were being performed on links that are downstream from the selected links that the provisioned monitor is disposed on ... .

Claim 7 is also allowable for analogous reasons as in claims 1 and 11. Claims 8-10 provide additionally distinct features, as of record.

Claim 24 is allowable since Ioele fails to suggest much less describe ... collecting statistical information for a plurality of provisioned customers on links that are downstream from links on which collecting occurs and maintaining separate counter logs for each provisioned customer; and a global counter log that accounts for all traffic seen on the links on which collecting occurs. Claims 25-27 (formally claims 25, 27 and 28) are allowable with claim 24.

Claim 28 (formally claim 29) is allowable with claim 7. In addition, claim 28 further distinguishes since it includes the additional feature of ... performing traffic analysis on the collected statistical information on a per downstream link basis to identify malicious traffic and communicating alerts that arise from the traffic analysis. Ioele fails to suggest statistical information and fails therefore to at least perform traffic analysis based on collected statistical information. Claims 29-33 are allowable with claim 28.

Entry of the above amendments is respectfully requested since the amendments correct minor typographical errors pointed out by the examiner or renumber the claims, or clarify language used in the claims.

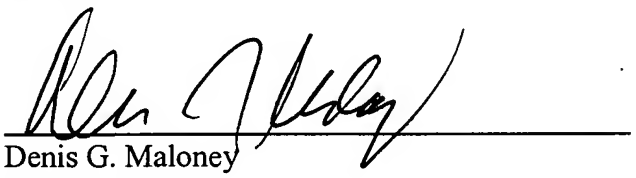
For example, in claim 3 "statistics" was deleted and replaced with "the statistical information on packets," which has antecedent basis in the base claim. These amendments do not require but minor consideration and no additional search by the examiner and place the application in condition for allowance and in better form for appeal by materially reducing the issues on appeal.

This Reply is accompanied by a Notice of Appeal.

Please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 8/14/06



Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21388347.doc